15. Wahlperiode

Drucksache **15/1538**

HESSISCHER LANDTAG

30. 08. 2000

Stellungnahme der Landesregierung

betreffend den Achtundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Drucksache 15/1101

Eingegangen am 30. August 2000 · Ausgegeben am 7. September 2000

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Zu 1
Vorwort

Auch der 28. Tätigkeitsbericht bietet der Landesregierung nahezu keinen Anlass für Auseinandersetzungen mit dem Hessischen Datenschutzbeauftragten, sodass sie sich in ihrer Stellungnahme wie in den Jahren zuvor auf wenige Anmerkungen beschränken kann. Diese Beschränkung kann nur bei oberflächlicher Betrachtung zu dem Missverständnis führen, die Kürze der Stellungnahme zeuge von einem geringen Interesse für den Datenschutz. Vielmehr ist das Gegenteil der Fall, weil gerade der hohe Stellenwert, den die Landesregierung dieser Aufgabe beimisst, zu einer weitgehenden Übereinstimmung mit dem Datenschutzbeauftragten führt. Da in Hessen das Verhältnis zwischen ihm und der Landesregierung von Anfang an nicht auf Konfrontation, sondern auf konstruktive Zusammenarbeit gerichtet war, kommt den Tätigkeitsberichten in diesem Lande vor allem eine informative Aufgabe zu. Zum einen enthalten sie im Zusammenhang mit Gesetzgebungsverfahren wichtige Anregungen für Exekutive und Legislative, wie die Ausführungen zu dem am 16. Mai 2000 vom Landtag beschlossenen Vierten Gesetz zur Änderung des HSOG zeigen. Zum anderen dienen die Berichte einer flächendeckenden Umsetzung der gesetzlichen Datenschutzvorschriften. Gerade dieser Aufgabe kommt eine besondere Bedeutung zu, da die Dezentralisierung und der rasch zunehmende Umfang der automatisierten Datenverarbeitung eine zentrale Kontrolle und Beratung zunehmend erschweren. Um diesen Schwierigkeiten zu begegnen, hat der hessische Gesetzgeber bereits 1986 als Erster die dezentrale Einrichtung behördlicher Datenschutzbeauftragter zur Stärkung des Datenschutzes vor Ort zwingend vorgeschrieben und deren Stellung bei der Novellierung 1998 erheblich gestärkt. Für die behördlichen Datenschutzbeauftragten stellen die jährlichen Tätigkeitsberichte mit ihren anschaulichen Beispielsfällen eines der wichtigsten Hilfsmittel dar. Die moderne Datenverarbeitungstechnik, deren gesetzeskonforme Nutzung die behördlichen Datenschutzbeauftragten einerseits kontrollieren sollen, kann von ihnen andererseits zur Erleichterung dieser Kontrollen genutzt werden. So bietet ihnen das Internet die Möglichkeit, die dort eingestellten Tätigkeitsberichte jederzeit abzurufen und gezielt auszuwerten.

Die präventive Aufgabe der Unterrichtung und Sensibilisierung durch Beispiele wird im nicht-öffentlichen Bereich durch den zusammen mit dieser Stellungnahme abgegebenen Bericht der Landesregierung über die Aufsichtstätigkeit der Regierungspräsidien erfüllt. Nutzer dieser Berichte sind auch im privatwirtschaftlichen Bereich vor allem die dezentralen betrieblichen Datenschutzbeauftragten der Unternehmen. Deren bundesweites Interesse an den Berichten und ihre positiven Rückmeldungen lassen seit Jahren den Schluss zu, dass in diesen Kreisen die Tätigkeit der Regierungspräsidien beachtliche Anerkennung findet. Dabei ist zu berücksichtigen, dass die Probleme vor allem im informationstechnisch hoch entwickelten Ballungsraum des Rhein-Main-Gebietes weitaus zahlreicher und komplizierter sind als im behördlichen Bereich. Es ist deshalb zu begrüßen, dass der Hessische Datenschutzbeauftragte die Übertragung der Datenschutzkontrolle über die Privatwirtschaft auf ihn nicht mit der Begründung gefordert hat, die Regierungspräsidien würden ihre Aufgabe nicht so gut erfüllen, wie es einer zentralen Kontrollstelle bei einer umfangreichen und problembeladenen dezentralen Datenverarbeitung überhaupt möglich ist. Vielmehr begründet der Hessische Datenschutzbeauftragte seine Forderung im Vorwort mit der "Auslegung der (EG-Datenschutz) Richtlinie, wonach die Datenschutzkontrollstellen für alle Bereiche funktional und institutionell unabhängig anzusiedeln sind". Wie die Landesregierung bereits 1998 in ihrer Stellungnahme zum 26. Tätigkeitsbericht (Drucks. 14/4167, S. 3) ausgeführt hat, überzeugt diese Begründung jedoch nicht, da die Richtlinie nur eine funktionale und keine institutionelle Unabhängigkeit fordert. Der frühere Hessische Datenschutzbeauftragte, Professor Dr. Simitis, der an der Entstehung der Richtlinie in Brüssel beteiligt war, macht dies in der Einleitung seines Kommentars zur Richtlinie (Rdnr. 40) wie folgt deutlich: "Die Kommission hatte allerdings um der Unabhängigkeit willen eine klare institutionelle Trennung verlangt, wie sie für die Datenschutzbeauftragten in der Bundesrepublik oder die Commission Nationale de I'Informatique et des Libertés in Frankreich typisch ist. Der Rat hat es abgelehnt, sich ähnlich deutlich festzulegen. Die Inkorporation der Kontrollinstanz in die öffentliche Verwaltung ist deshalb, für sich genommen, noch kein Verstoß gegen die Richtlinie. Vielmehr kommt es darauf an, ob eine funktionale Trennung, wie etwa in Dänemark, gesetzlich sowie organi-

satorisch abgesichert und zugleich die Unabhängigkeit der Kontrollinstanz unmissverständlich garantiert ist." In demselben Kommentar führt der Mitkommentator Dr. Dammann zu Art. 28 (Rdnr. 5) aus: "Bis zum geänderten Vorschlag hatte die Richtlinie die Unabhängigkeit schlicht als Attribut der Kontrollstelle gefordert (eine unabhängige staatliche Behörde). Mit Rücksicht auf einige Mitgliedstaaten, nach deren Auffassung diese Formulierung zu weitgehende Interpretationen eröffnete, wählten Kommission und Rat im gemeinsamen Standpunkt die schließlich in die Richtlinie aufgenommene Formulierung, die das Merkmal der Unabhängigkeit nicht der Institution als solcher direkt zuschreibt, sondern die Unabhängigkeit als ein Merkmal der Aufgabenwahrnehmung ausweist."

Die somit allein entscheidende Garantie der funktionalen Unabhängigkeit bei der Aufgabenwahrnehmung ist inzwischen auf einhelligen Wunsch der Bundesländer in § 38 Abs. 1 des Referentenentwurfs vom 7. April 2000 zur Anpassung des Bundesdatenschutzgesetzes an die EG-Richtlinie aufgenommen worden. Danach ist festgelegt, dass alle bei der Kontrolltätigkeit gewonnenen Erkenntnisse ausschließlich für Zwecke der Aufsicht verwendet werden dürfen. Damit ist die Aufsichtsbehörde abgeschottet und unabhängig von den Informationsinteressen der übrigen Verwaltung, ganz gleich, wo sie institutionell angesiedelt ist. Unter diesen Voraussetzungen ist es den Ländern in Übereinstimmung mit der Richtlinie freigestellt, ob sie die Regierungspräsidien oder die Datenschutzbeauftragten mit der Datenschutzkontrolle über die Privatwirtschaft betrauen. Die überwiegende Mehrheit der Flächenländer hat nicht die Absicht, die Aufsicht auf die Datenschutzbeauftragten zu übertragen. In seinem Vorwort ist der Hessische Datenschutzbeauftragte einerseits der Auffassung, dass die Kontrolle über die Privatwirtschaft im "ministerialfreien Raum" bei seiner Behörde "verselbstständigt und weisungsfrei" zu institutionalisieren sei, tritt aber andererseits dafür ein, dass Hessen "der in einigen Bundesländern bereits vollzogenen Neuordnung folgen möge". Der Gesetzgeber in Nordrhein-Westfalen hat jedoch gerade erst durch Gesetz vom 13. April 2000 die Kontrolle über die Privatwirtschaft zwar der Landesbeauftragten übertragen, es aber aus verfassungsrechtlichen Gründen für geboten erachtet, sie insoweit den Weisungen des Innenministeriums zu unterstellen. Auch das durch Gesetz vom 25. November 1999 in Schleswig-Holstein errichtete Unabhängige Landeszentrum für Datenschutz untersteht der Rechtsaufsicht des Innenministeriums.

Wegen der schwerwiegenden verfassungsrechtlichen Bedenken beabsichtigt kein Bundesland, die mit weitreichenden Exekutivbefugnissen verbundene Datenschutzkontrolle über die Privatwirtschaft dem Datenschutzbeauftragten als weisungsfreie Aufgabe zu übertragen.

Zu 5
Polizei- und Strafverfolgungsbehörden

Zu 5.2
Durchführung von DNA-Analysen

Die gegen die Durchführung der molekulargenetischen Untersuchung auf der Grundlage einer Freiwilligkeitserklärung des Betroffenen vorgebrachte Kritik war bereits Gegenstand des 27. Tätigkeitsberichtes des Hessischen Datenschutzbeauftragten. Die Hessische Landesregierung vermag gleichwohl ihren hierzu bisher eingenommenen Standpunkt nicht zu revidieren und sieht sich im Übrigen durch die mittlerweile hierzu ergangenen Entscheidungen des Landgerichts Stralsund vom 3. Juni 1999 (III Qs 96/99), des Landgerichts Berlin vom 5. November 1999 (522 Qs 118/99) sowie des Landgerichts Hamburg vom 17. November 1999 (628 Qs 46/99) und vom 24. November 1999 (611 Qs 102/99) bestätigt.

Klarzustellen ist nochmals, dass die Regelung der §§ 81e, 81f, 81g StPO und des § 2 DNA-Identitätsfeststellungsgesetz materielle und verfahrensrechtliche Vorgaben für einen Eingriff in das Recht auf informationelle Selbstbestimmung enthalten. Wenn und soweit der Betroffene in die Entnahme seiner Körperzellen (Speichelabstrich) und deren molekulargenetischen Untersuchung einwilligt, findet ein solcher staatlicher Eingriff nicht statt, wie sich aus dem Begriff der Selbstbestimmung unmittelbar ergibt. Danach entfällt durch eine Einwilligung des Betroffenen die Notwendigkeit eines gerichtlichen Verfahrens zur Erhebung des DNA-Fingerprints insgesamt. Zutreffend ist, dass dieses Argument lediglich die

genau dies aber ist der ausschließliche Gegenstand des Richtervorbehaltes in §§ 81f, 81e und 81g StPO, § 2 DNA-Identitätsfeststellungsgesetz, während die Speicherung der Daten bei dem Bundeskriminalamt auf der Grundlage des § 8 BKAG erfolgt.

Zwar trifft es zu, dass der Wortlaut des § 81a Abs. 1 Satz 2 StPO für die Zellenentnahme explizit die Möglichkeit der Einwilligung vorsieht - anders als dies in den Vorschriften der §§ 81e, 81f, 81g StPO der Fall ist. Jedoch schützt jene Vorschrift nicht das Recht auf informationelle Selbstbestimmung, sondern vielmehr die körperliche Unversehrtheit. Dieses Rechtsgut besteht - abgesehen von der in den Grenzen des § 228 StGB freilich auch insoweit gegebenen Dispositionsbefugnis - nicht in der Selbstbestimmung über den eigenen Körper, sondern in dessen Unverletztheit als solcher. In dieser Unterschiedlichkeit der betroffenen Rechtsgüter mag sich auch die divergierende Berücksichtigung der Einwilligung des Betroffenen im Wortlaut des § 81a StPO einerseits und der §§ 81f, 81g StPO andererseits rechtfertigen. Klarzustellen ist aber, dass die StPO auch an anderer Stelle die Einwilligung des Betroffenen nicht im Gesetzeswortlaut thematisiert, gleichwohl aber von der Entbehrlichkeit der richterlichen Anordnung insoweit ausgegangen wird. Als Beispiel mag auf die §§ 102, 103, 105 StPO hingewiesen werden. Die Strafverfolgungsbehörden sind mit Einverständnis des Berechtigten auch ohne richterlichen Beschluss zur Durchsuchung von Wohnräumen befugt - es ist unstreitig, dass bei Vorliegen des Einverständnisses ein Eingriff in das durch Art. 13 GG sowie § 123 StGB geschützte Rechtsgut nicht vorliegt.

Den im Tätigkeitsbericht aus der Verweisung des § 81g Abs. 3 nur auf § 81a Abs. 2 StPO (und nicht auch auf Abs. 1 der Vorschrift) gezogenen Schlüssen vermag die Hessische Landesregierung nicht beizutreten. Diese beschränkte Verweisung begründet sich ausschließlich in dem Umstand, dass allein die Verfahrensregelung des § 81a Abs. 2 StPO und nicht zugleich die materielle Eingriffsnorm des Abs. 1 der Vorschrift in Bezug genommen werden soll - wie auch die weitere Verweisung lediglich § 81f StPO und nicht auch § 81e StPO erfasst. Rückschlüsse auf die Konsequenzen einer Einverständniserklärung des Betroffenen lassen sich hierdurch nicht begründen.

Vorbehalte gegen den Umfang der Belehrung, vermutete Defizite im Verständnis des Betroffenen hinsichtlich der Reichweite der von ihm abgegebenen Erklärung oder generelle Zweifel an der Entscheidungsfreiheit von Strafgefangenen betreffen allein die aufgrund der Umstände des Einzelfalles zu bewertende Frage, ob ein Einverständnis des Betroffenen in die Untersuchung auch tatsächlich gegeben ist, nicht hingegen die grundsätzliche Zulässigkeit einer diesbezüglichen Disposition des Betroffenen als Inhaber des informationellen Selbstbestimmungsrechts. Die entsprechende Belehrung des Betroffenen beruht in Hessen auf einem Formular, das vom Hessischen Landeskriminalamt unter Mitwirkung des Hessischen Datenschutzbeauftragten entwickelt worden ist. In dem Vordruck ist eine Belehrung nicht nur über die Zellentnahme und deren Untersuchung, sondern explizit auch hinsichtlich der Speicherung der Identifizierungsmuster in der Datei des Bundeskriminalamtes und deren Zweck vorgesehen. Die Hessische Landesregierung ist der Auffassung, dass damit den zu stellenden Anforderungen in angemessener Weise Rechnung getragen wird.

Zu 5.2.2
Handhabung der DNA-Analysen zum Zwecke der Identitätsfeststellung beim Landeskriminalamt

Um den Dienststellen nach der Erweiterung der gesetzlichen Befugnisse ein Hilfsmittel für die Bearbeitung von DNA-Fällen an die Hand zu geben, hat das HLKA am 1. Juli 1999 "Richtlinien zur DNA-Analyse-Datei" erarbeitet. Die vom Hessischen Datenschutzbeauftragten gesehenen Probleme wurden mit ihm am 26. August 1999 erörtert und, wie er dem HLKA am 22. Dezember 1999 bestätigte, bereinigt. Die abgeänderten Richtlinien wurden am 8. Juni 2000 an die Dienststellen verschickt.

Soweit der Datenschutzbeauftragte die Auffassung vertritt, es sei unzulässig, eine Person, die als Spurenleger nicht ausgeschlossen werden könne, zum Beschuldigten zu machen, ist ihm beizupflichten. Nur derjenige darf die Stellung eines Beschuldigten erhalten, in dessen Person sich ein Tatverdacht konkretisiert hat. Dieser Tatverdacht wird sich in der Regel aus anderen

Umständen als den am Tatort aufgefundenen DNA-Spuren ergeben. Die Richtlinien gelten im Übrigen ausdrücklich nicht für Reihenuntersuchungen auf freiwilliger Basis, bei denen der zu untersuchende Personenkreis mangels Tatverdachts durch Ausschlusskriterien festgelegt wird.

Zu 5.3
Polizeiliche Datenspeicherung trotz Freispruch

Der vom Hessischen Datenschutzbeauftragten dargestellte Sachverhalt ist zutreffend. Die Angelegenheit wurde bereits am 16. Juli 1999 zwischen einem seiner Mitarbeiter und dem Datenschutzbeauftragten des Polizeipräsidiums Frankfurt am Main erörtert. Noch am gleichen Tag wurden die festgestellten Unrichtigkeiten bei der Sachbearbeitung der zuständigen Organisationseinheit mitgeteilt und die Löschung der über den Betroffenen gespeicherten Daten und die Vernichtung der Kriminalakte veranlasst.

Der behördliche Datenschutzbeauftragte hat zur Vermeidung ähnlicher Vorfälle in der Zukunft eine interne Nachbearbeitung des Vorgangs veranlasst.

Zu 6
Justiz und Strafvollstreckung
Elektronische Fußfessel

Die Hessische Landesregierung stimmt mit den Ausführungen im Tätigkeitsbericht weitestgehend überein. Klarzustellen ist, dass der Modellversuch in Frankfurt am Main den Einsatz der "elektronischen Fußfessel" in erster Linie im Rahmen einer Weisung bei Strafaussetzung zur Bewährung zum Gegenstand hat. In der Diskussion um eine Änderung des Strafvollzugsgesetzes hingegen wird tatsächlich um eine andere Form der Freiheitsstrafe bzw. um eine andere Form deren Vollzuges gerungen - dies ist nicht Gegenstand des hiesigen Modellversuchs. Die Hessische Landesregierung sieht daher auch kein Junktim zwischen einer diesbezüglichen Entscheidung des Deutschen Bundestags und dem hier durchgeführten Projekt.

Zu 10
Entwicklungen im Bereich der Technik

Zu 10.1
Fallstricke bei der Benutzung von E-Mail

Zu 10.1.1
Ablaufskizze

Neben der Verarbeitung von E-Mails über einen entsprechenden, auf dem Arbeitsplatzsystem installierten E-Mail-Client wird von vielen Anbietern (oftmals ergänzend) auch die Bearbeitung (Lesen/Erstellen etc.) von E-Mails über eine Browser-Oberfläche angeboten (z.B. Freenet, GMX). Bei einer derartigen Verfahrensweise ist das Gefahrenpotenzial naturgemäß anders als bei der vom HDSB dargelegten Mail-Client-Lösung.

Zu 10.1.2.1
Unbefugte Kenntnisnahme des Passwortes

Das IMAP4-Protokoll wird nur von wenigen Providern unterstützt. Bei IMAP4 bleiben die Mails standardmäßig auf dem Mail-Server des Providers und werden nicht auf den Client-Rechner des Benutzers kopiert. Dadurch kann es zu Kapazitätsproblemen hinsichtlich des notwendigen Plattenplatzes auf dem Mail-Server des Providers kommen. Damit greifen dann wieder die unter 10.1.2.3 geschilderten Probleme (Unbefugtes Löschen von Nachrichten).

Zu 10.1.2.2
Unbefugte Kenntnisnahme der E-Mail während der Übertragung oder der Speicherung auf den Servern

Derzeit wird in der HZD die notwendige Infrastruktur (Client-Software und Keyserver) zum Betrieb einer PGP-basierten Sicherheitsinfrastruktur in der HZD aufgebaut, wobei eine Erweiterung auf die hessische Landesverwaltung beabsichtigt ist.

Zu 10.1.2.7
Schadprogramme

Neben der Schädigung des Client-Rechners legen einige Schadprogramme (z.B. "Melissa" oder jetzt aktuell "ILOVEYOU" bzw. "LOVELETTER-FOR-YOU") aufgrund ihres Verteilmechanismus auch Mail-Server in Firmen und bei Providern lahm.
Ein ähnliches Ziel verfolgen auch die so genannten "HOAX"-mails. Darin wird der Empfänger aufgefordert, diese "Warnung" vor einem besonders gefährlichen Virus unbedingt an alle Bekannten weiterzugeben. Die Viren, vor denen in diesen Mails gewarnt wird, sind aber nicht existent (eben "hoax"). Allein das massenhafte Verteilen der Virenwarnung kann aber zu Abstürzen von Mail-Servern durch Überlastung führen. Recht gute Übersichten über diese HOAX werden von NAI oder der TU Berlin im Internet zur Verfügung gestellt.
Es soll hier aber nicht ein sorgloser Umgang mit Virenwarnungen propagiert werden. Im Gegenteil - jede Virenwarnung sollte zunächst ernst genommen und anhand aktueller "HOAX"-Listen geprüft werden (so z.B. geschehen bei Loveletter). Allerdings sollte eine unkontrollierte Weiterverteilung der Mails vermieden werden.

Zu den Möglichkeiten eines zentralen Mobile-Code-Scannings wird derzeit in der HZD ein Projekt durchgeführt. Für den Teilbereich Virenscanning wurde das Projekt bereits im Jahr 1999 weitgehend abgeschlossen, für das Jahr 2000 stehen hierzu die Beschaffung sowie die Installation/Konfiguration an. Für den Teilbereich Java und Javascript-Scanning ist abschließend ein letzter Test mit einem unter Federführung des BSI entwickelten Produkt geplant.

Zu 10.2
Fernadministration und Fernwartung von Firewalls

Unter 10.2.1 wird die Forderung erhoben, dass der Betreiber Know-how vorhalten muss, um die Fernadministration "technisch und vom Wissen her" zu kontrollieren. Dies wird de facto jedoch zu erheblichen Problemen führen, da der Betreiber i.d.R. gerade aufgrund mangelnden fachlichen Know-hows zum Outsourcing veranlasst wurde. Hier bietet es sich an, Dienstleistungen externer Dienstleister in Anspruch zu nehmen, die selbst Teil der Verwaltung sind (z.B. HZD).

Bei der Bestimmung des Umfangs der Zugriffsrechte ist es sinnvoll, grundsätzlich von einem "Least Privilege" Prinzip auszugehen. Es werden somit nur geringste Rechte, die zur Erfüllung der Aufgabe notwendig sind, vergeben.
Die Einleitung der Fernadministration durch den Betreiber kann bei spontan auftretenden Problemen schwierig sein, da der Fernadministrator zumeist auch die Überwachung des Systems durchführt.

Zu 14
Soziales

Zu 14.2
Täter-Opfer-Ausgleich bei Jugendlichen

Die hier wiedergegebene Kontroverse dürfte sich im Wesentlichen durch das Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des Gesetzes über Fernmeldeanlagen vom 20. Dezember 1999 (BGBl. Teil 1, 1999, S. 2491) erledigt haben. § 155b Abs. 1 StPO enthält hierzu folgende Regelung:

"(1) Die Staatsanwaltschaft und die Gerichte können zum Zweck des Täter-Opfer-Ausgleichs oder der Schadenswiedergutmachung einer von ihnen mit der Durchführung beauftragten Stelle von Amts wegen oder auf deren Antrag die hierfür erforderlichen personenbezogenen Informationen übermitteln. Die Akten können der beauftragten Stelle zur Einsichtnahme auch übersandt werden, soweit die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern würde. Eine nicht-öffentliche Stelle ist darauf hinzuweisen, dass sie die übermittelten Informationen nur für Zwecke des Täter-Opfer-Ausgleichs oder der Schadenswiedergutmachung verwenden darf."

Damit sind die Übermittlungsbefugnisse der Staatsanwaltschaft gegenüber den mit der Durchführung des Täter-Opfer-Ausgleichs beauftragten Stellen bereichsspezifisch geregelt. Die Vorschrift ist auch im Jugendstrafverfahren anzuwenden (§ 2 JGG).

Die Einbindung der Jugendämter bei der Vorbereitung und Durchführung des Täter-Opfer-Ausgleichs ist im Übrigen auch ein den strafprozessualen Vorschriften des JGG (§ 38 Abs. 3) zu entnehmendes Gebot.

Zu 23
Bilanz

Zu 23.1
Medizinische Daten in Ausländerakten

Der mit dem Datenschutzbeauftragten abgestimmte Erlass über medizinische Daten in Ausländerakten ist den Ausländerbehörden am 14. September 1999 zugeleitet worden.

Zu 24
Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Zu 24.5
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17. Juni 1999
Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

Zu der Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17. Juni 1999 ist aus der Sicht der Hessischen Landesregierung Folgendes zu bemerken:

Die Frage, ob sich das Gebot der Gewährleistung einer gleichwertigen parlamentarischen Kontrolle für Maßnahmen der Wohnraumüberwachung in den Ländern auch auf strafprozessuale Maßnahmen nach § 100c Abs. 1 Nr. 3 StPO erstreckt, ist durchaus umstritten. Aus dem Zusammenspiel der Nachschaltung von Richtervorbehalt und parlamentarischer Kontrolle einerseits und dem Prinzip der Gewaltenteilung andererseits spricht einiges dafür, dass die Berichtspflicht des Art. 13 Abs. 6 GG primär als legislative Selbstkontrolle zur Schaffung und Sicherung empirischer Erkenntnisquellen für den Gesetzgeber und daher nicht als eine unmittelbare Kontrolle exekutiver Umsetzungen zu verstehen ist. Eine Kontrolle im letzteren Sinne würde sich nämlich tatsächlich weniger als Kontrolle der Strafverfolgungsbehörden denn als unmittelbare Kontrolle und Kritik der Spruchpraxis der zuständigen Gerichte auswirken. Versteht man die Kontrolle des Art. 13 Abs. 6 GG daher lediglich als Selbstkontrolle der Parlamente im Hinblick auf eine Überprüfung der geltenden Vorschriften sowie eines gegebenebfalls bestehenden legislativen Handlungsbedarfes, so orientiert sich die Berichtspflicht nach den Regelungskompetenzen der jeweiligen Gesetzgebungskörperschaft. Danach wäre dem Hessischen Landtag lediglich über die auf der Grundlage des HSOG sowie des Landesverfassungsschutzrechtes durchgeführten Maßnahmen, nicht aber über die repressive Wohnraumüberwachung nach der StPO zu berichten.

Unabhängig von der somit durchaus bestreitbaren Frage bestehender Rechtspflichten entspricht es jedoch der Praxis der Hessischen Landesregierung, der Artikel-13-Grundgesetz-Kommission aus Achtung vor der parlamentarischen Autonomie des Landtags auch über die Praxis der Wohnraumüberwachung zu Zwecken des Strafverfahrens nach § 100c Abs. 1 Satz 3 StPO zu berichten. Hierzu teilt das Hessische Ministerium der Justiz jeweils nach dem Ende des ersten Quartals eines Jahres die Ergebnisse der von den Landesjustizverwaltungen vereinbarten anonymisierten und standardisierten Zählungen mit, wie sie auch an das Bundesministerium der Justiz übermittelt werden.

Wiesbaden, 25. August 2000

Der Hessische Ministerpräsident
Koch

Der Hessische Minister des Innern und für Sport
Bouffier